UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN
MILWAUKEE DIVISION

Deanna Danger, *On Behalf of Herself and Those Similarly Situated*, Plaintiff, v. Advocate Aurora Health, Inc., Defendants.	Case No. Judge **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Deanna Danger, individually and on behalf of all others similarly situated ("Plaintiffs") bring this Class Action Complaint against Advocate Aurora Health, Inc. ("Advocate" or "Defendant"), and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and to safeguard personally identifiable information and personal health information (collectively referred to herein as "Private Information"), including, but not limited to, names, email addresses, phone numbers, computer IP addresses, emergency contact information, appointment information, medical provider information, medical histories, and other content submitted on Defendant's

website and patient portal.[1]

2. Defendant is a health care network with its corporate headquarters in in Milwaukee, Wisconsin. In 2021, Defendant's healthcare network included 27 hospitals and more than 500 sites of care. Defendant also employed 75,000 individuals, including 10,000 employed physicians.[2]

3. Defendant knowingly configured and implemented a Tracking Pixel ("Pixel") to collect and transmit information from its website to third parties, including information communicated in sensitive and presumptively confidential patient portals and mobile apps like its MyChart portal and LiveWell app.[3]

4. Defendant acknowledged to the over 3,000,000 individuals whose information was compromised that it designed the Tracking Pixel to transmit its patients IP addresses; the dates, times, or locations of scheduled appointments; their proximity to an Advocate Aurora Health location when using the site; information about medical providers; the nature of appointments and medical procedures; communications between patients and Advocate through MyChart, and first and last names, medical record numbers, and insurance information (collectively "Private Information").[4]

5. Plaintiff's lawsuit arises out of Defendant's choice to install the Facebook tracking pixel and other tracking software on its web properties and to configure it to allow Defendant and its marketing partners to gather and to analyze various analytics based on the information collected from visitors to the sites.

---

[1] https://www.advocateaurorahealth.org/pixel-notification/ (last visited: November 3, 2022).
[2] *See supra* Fn. 1.
[3] https://www.jsonline.com/story/news/2022/10/21/advocate-aurora-health-data-breach-could-impact-3-million-patients/69581723007/ (last accessed: October 27, 2022).
[4] https://www.healthcareitnews.com/news/advocate-aurora-notifies-patients-potential-tracking-pixel-breach (last accessed October 27, 2022).

6. A Pixel is a piece of code that organizations commonly use for marketing purposes like measuring activity and enhancing experiences on web properties.

7. The tracking pixel operates by embedding invisible code in each page a visitor views on the website. The code within the tracking pixel captures the information including the webpage name, visitors' interactions with the page (including which buttons they click and information they enter into form fields e.g., home address, phone number, email address, and medical information concerns treatment history), search queries, visitors' IP addresses, and browser identifiers.[5] The code then transmits the information both to Facebook and Defendant to use for their respective business purposes and, generally speaking monetary gain.

8. Plaintiff did not permit or give authorization for Defendant to disclose their Private Information and intercept communications they believed and understood to be confidential and only between themselves and their healthcare provider. Plaintiffs were never provided with any written notice that Advocate discloses its website users' protected health information, nor were Plaintiffs provided any means of opting out of such disclosures. Despite this, Advocate knowingly disclosed Plaintiffs' protected health information to Facebook.

9. Defendant did not disclose that it had transmitted patients' sensitive and non-public Private information to unauthorized third parties until on or around October 20, 2022, when it sent Notice of Data Breach letters ("Notice") and posted a notice on its website.

10. Healthcare organizations, like Defendant, that collect and store Private Information have statutory, regulatory, contractual, and common law duties to safeguard that information and to ensure it remains private. Healthcare providers, like Defendant, have a fiduciary duty to keep their patients' Private Information confidential and protected from disclosure.

[5] https://developers.facebook.com/docs/meta-pixel/ (last accessed: October 27, 2022).

11. Event though Defendant had a duty to maintain Plaintiff's and Class Members' Private Information as confidential, Defendant knowingly implemented tracking software that collects and discloses Private Information to third parties for business purposes.

12. Defendant's unlawful tracking and disclosure of Plaintiff's and Class Members' Private Information is an egregious breach of their duty.

13. Plaintiff and Class Members relied upon Defendant to maintain the security and privacy of the Private Information they entrusted to it.

14. Plaintiff and Class Members reasonably expected and understood that Defendant would comply with its obligations to keep their Private Information secure and safe from unauthorized access and disclosure.

15. The Data Breach is a direct result of Defendant's actions because Defendant knowingly implemented and configured the pixel to disclose the identities and communications of its patients to Meta Platform, Inc. d/b/a Facebook ("Meta" or "Facebook").

16. Meta's get started page clearly discloses that the pixel "relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can tally their actions in the Facebook Ads Manager so you can use the data to analyze your website's conversion flows and optimize your ad campaigns."[6] Accordingly, Defendant chose to incorporate code on its website knowing that the code was intended to specifically identify its patients to Facebook alongside their protected health information and geographic location.

17. Plaintiff brings this action, individually and on behalf of all persons, whose Private Information was compromised as a result of Defendant's knowing and willful disclosure of it patients' Private Information.

[6] https://developers.facebook.com/docs/meta-pixel/get-started (last accessed: October 27, 2022).

18. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently disclosing its patients' Private Information via the tracking Pixel. As a result, Plaintiff and Class Members' Private Information was compromised through disclosure to Meta, Facebook, Goggle, and other unknown and unauthorized third parties. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains confidential and disclosed only according to a patient's authorization, and they should be entitled to injunctive and other equitable relief.

PARTIES

19. Plaintiff Deanna Danger is a citizen and resident of Milwaukee, Wisconsin.

20. Defendant Advocate Aurora Health is a not-for-profit corporation incorporated in Delaware with its principal place of business at 750 W. Virginia St. P.O. Box 341880, Milwaukee, Wisconsin 53204.

JURISDICTION AND VENUE

21. This Court has subject matter and diversity jurisdiction over this action under 28U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

22. The Eastern District of Wisconsin has personal jurisdiction over the Defendant named in this action because one of Defendant's headquarters is in this District and Defendant conducts substantial business in this District through its headquarters, offices, parents and/or affiliates.

23. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant

and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Background

24. Defendant is a large health network with locations in Wisconsin and Illinois.

25. Defendant uses digital platforms like MyChart and LiveWell platforms to serve many of its patients.

26. Defendant's digital platforms enable patients to schedule appointments or procedures, communicate with their healthcare providers, review their medical histories, and perform other healthcare focused communications.

27. Plaintiff and Class Members relied on the sophistication of Defendant's healthcare business to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

28. The Pixel and other tracking software that Defendant installed on its healthcare portals tracks users as they navigate through the website and applications and logs which pages are visited, which buttons are clicked, specific information users enter into forms (e.g., name, home address, phone number, email address), search queries (e.g., "do I have covid"), and information including a patient's IP address.[7]

29. As more fully explained below, this information is collected by *both* Defendant and Meta. Specifically, the Pixel Defendants embeds into its website simultaneously transmits all the

[7] *See supra* Fn. 5.

information it receives to Meta.[8]

30. If the patient is also a Meta user, then Meta, in turn, links the information they receive to the patient's Meta profile, which includes other identifying information.

31. Defendant strongly encourages patients to use digital tools, which then Defendant tracks via the pixel tracking code.

32. For example, Defendant promised its patients that "the LiveWell with Advocate Aurora Health app and website are secure environments. For more information, see our privacy policy."[9]

33. Defendant's Privacy Policy applies to any personal information provided to Advocate and any personal information that Advocate collects from other sources.

34. Defendant's Privacy Policy does not permit Defendant to use and disclose Plaintiffs' and Class Members' Private Information for marketing purposes without written permission.

35. Defendant violated its own Privacy Policy by unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook, Meta, Google, and likely other third parties.

36. Its Privacy Policy states: "Examples of how you might provide us with such personal information include:

- Completing a survey or feedback form;
- Email us with a comment or question;
- Subscribing to our email notification service for new editions of Health Advocate magazine;
- Establishing a personalized homepage via our website;
- Making an online appointment / requestion an appointment;

[8] Defendant acknowledges that the tracking software it implemented on its website likely disclosed the Private Information to Google and other companies.
[9] http://web.archive.org/web/20211220195147/https://www.advocateaurorahealth.org/livewell/faq#security-sign-in (as reflected on December 21, 2021)

- Engaging in an online dialogue via chat; Completing an online bill payment;
- Scheduling and/or use of Virtual Visits;
- Preforming online check-in; and
- Using site-based wayfinding functions.

…

Our web server automatically collects and records the following information:

- Aggregate information on what pages are accessed;
- Address of the website that linked to us (referral URL);
- Date and time you access our site;
- Name and release number of web browser software used;
- Operating system used;
- Visitor's domain name, but not the email address; Visitor's IP address; and
- Age, gender and interests.

…

This site recognizes and collects, when possible, the domain name of a visitor's server (for example, advocatehealth.com or aol.com). We do not automatically collect the full email address of visitors to our website. The only way we obtain your name or email address is when you choose to provide that information to us. Examples of how you might provide us with such personal information include:

- Completing a survey or feedback form;
- Email us with a comment or question;
- Subscribing to our email notification service for new editions of Health Advocate magazine; and
- Establishing a personalized homepage via our website.

…

How do we use the information we collect? Advocate Health Care does not sell, trade or rent personal information about its website visitors.

…

Information provided to schedule online appointment, pay online bills, chat, virtual visits and other web functions may be transferred to 3rd party vendors and partners to continue service.

...

Data collection
You may browse many areas of our website, including our home page, without

disclosing any personal information about yourself. Within these areas we only collect and store the information that is automatically recognized by the Web server, such as your IP address and files you request from the server.

…

We collect the personal data that you volunteer on registration(s), survey, online chat, online bill pay, virtual/telehealth visits, or other forms, or by email. Additionally, some areas of our website might be available only to certain persons and will require a login and password to access these areas. In order to be granted a login and password you may be asked some demographic information about yourself.

…

Data analysis
As described above, we sometimes collect anonymous information from visits to our site to help us provide better customer service. For example, we measure visitor activity on our website, but we do so in ways that keep the information anonymous. We use the information that we collect to measure the number of visitors to the different areas of our site and to help us make our site more useful to visitors. This includes analyzing these logs periodically to measure the traffic through our servers, the number of pages visited and the level of demand for pages and topics of interest. The logs may be preserved indefinitely and used at any time and in any way to prevent security breaches and to ensure the integrity of the data on our servers.

…

Cookies & other technologies
We collect the anonymous information we mentioned above through the use of various technologies, one of which is called "cookies". A cookie is an element of data that the website can send to your browser, which may then be stored on your hard drive. Cookies may last for only a single session or may span multiple sessions. We use cookies to track user activity by our registered users. Finally, cookies are employed in other applications that require the storage of user data from one screen to the next."[10]

37. Defendant violated its own Privacy Policy by unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook, Meta, and likely other third parties. Defendant further misrepresented that it would preserve the confidentiality of their Private

[10] *Id.*

Information and the anonymity of their identities.

The Data Breach

38. On or around October 20, 2022, Defendant posted a "Breach Notification" on its website.

39. The Notice of Data Breach informed Plaintiff and Class Members (in substantially the same form) of the breach:

> "Advocate Aurora Health is writing to provide transparency in its previous use of the Internet tracking technologies, such as Google and Meta (Facebook), that we and many others in our industry had implemented to understand how patients and others interact with our websites. These technologies disclose certain details about interactions with our websites, particularly for users that are concurrently logged into their Google or Facebook accounts and have shared their identity and other surfing habits with these companies. When using some Advocate Aurora Health sites, certain protected health information ("PHI") would be disclosed in particular circumstances to specific vendors because of pixels on our websites or applications. Information about these technologies and steps that individuals may take to further protect their health information can be found in our FAQ.
>
> In an effort to deliver high quality services to its community, Advocate Aurora Health uses the services of several third-party vendors to measure and evaluate information concerning the trends and preferences of its patients as they use our websites. To do so, pieces of code known as "pixels" were included on certain of our websites or applications. These pixels or similar technologies were designed to gather information that we review in aggregate so that we can better understand patient needs and preferences to provide needed care to our patient population. We learned that pixels or similar technologies installed on our patient portals available through MyChart and LiveWell websites and applications, as well as on some of our scheduling widgets, transmitted certain patient information to the third-party vendors that provided us with the pixel technology. We have disabled and/or removed the pixels from our platforms and launched an internal investigation to better understand what patient information was transmitted to our vendors.
>
> Out of an abundance of caution, Advocate Aurora Health has decided to assume that all patients with an Advocate Aurora Health MyChart account (including users of the LiveWell application), as well as any patients who used scheduling widgets on Advocate Aurora Health's platforms, may have been affected. Users may have been impacted differently based on their choice of browser; the configuration of their browsers; their blocking, clearing or use of cookies; whether they have Facebook or Google accounts; whether they were logged into

> Facebook or Google; and the specific actions taken on the platform by the user.
>
> The following information may have been involved: your IP address; dates, times, and/or locations of scheduled appointments; your proximity to an Advocate Aurora Health location; information about your provider; type of appointment or procedure; communications between you and others through MyChart, which may have included your first and last name and your medical record number; information about whether you had insurance; and, if you had a proxy MyChart account, your first name and the first name of your proxy. Based on our investigation, no social security number, financial account, credit card, or debit card information was involved in this incident.
>
> We have disabled and/or removed tracking pixels on patient websites and applications, and we are continuing to evaluate how to further mitigate the risk of unauthorized disclosures of patient protected health information in the future. We will continue to monitor our information security systems and make improvements and enhancements where appropriate. To the extent any tracking technologies are proposed in the future, such technologies will be evaluated under Advocate Aurora's enhanced, robust technology vetting process consistent with our commitments to patient privacy."[11]

40. Defendant advised that the information potentially impacted in the Data Breach included:

> "…your IP address; dates, times, and/or locations of scheduled appointments; your proximity to an Advocate Aurora Health location; information about your provider; type of appointment or procedure; communications between you and others through MyChart, which may have included your first and last name and your medical record number; information about whether you had insurance; and, if you had a proxy MyChart account, your first name and the first name of your proxy. Based on our investigation, no social security number, financial account, credit card, or debit card information was involved in this incident."[12]

41. There is a potential that more information was disclosed to Meta, Facebook, Google, and others during the two years data was submitted to Meta from Defendant's system.

42. Facebook describes itself as a "real identity platform,"[13] meaning users are

[11] https://www.advocateauroraheath.org/pixel-notification/ (last accessed: October 27, 2022).
[12] *Id.*
[13] Sam Schechner and Jeff Horwitz, How Many Users Does Facebook Have? The Company Struggles to Figure It Out, WALL. ST. J. (last accessed October 2022).

allowed only one account and must share "the name they go by in everyday life."[14] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[15]

43. In 2021, Facebook generated $117 billion in revenue.[16] Roughly 97% of that came from selling advertising space.[17]

44. Facebook sells advertising space by highlighting its ability to target users.[18]Facebook can target users so effectively because it surveils user activity both on and off its site.[19] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[20] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[21]

45. Advertisers can also build "Custom Audiences."[22] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're

---

[14] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, *available at* https://www.facebook.com/communitystandards/integrity_authenticity.
[15] FACEBOOK, SIGN UP, https://www.facebook.com/
[16]FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor- news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx
[17] *Id.*
[18]FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706.
[19] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.
[20] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.
[21] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.
[22] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.

loyal customers or people who have used [their] app or visited [their] website."[23] With Custom Audiences, advertisers can target existing customers directly, and they can also build a "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[24] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools."[25]

46. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[26] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

47. The Business Tools are configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[27] Facebook's Business Tools can also track

---

[23] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.
[24] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328.
[25] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.
[26] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087.
[27] See FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; see also FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP,

other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[28] Advertisers can even create their own tracking parameters by building a "custom event."[29]

48. One such Business Tool is the Facebook Tracking Pixel which Defendant implemented on its digital platforms. Facebook offers this piece of code to advertisers, like Advocate, to integrate into their website. As the name implies, the Facebook Pixel "tracks the people and type of actions they take."[30] When a user accesses a website hosting the Facebook Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers. This second, secret transmission contains the original request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's websites – Defendant's own code, and Facebook's embedded code.

49. An example illustrates the point. Take an individual who navigates to Defendant's website and clicks on the "Check Symptoms & Find COVID-19 Care" tab. When that tab is clicked, the individual's browser sends a request to Defendant's server requesting that server to load the particular webpage. Because Advocate utilizes the Facebook Pixel, Facebook's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, without

---

https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[28] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.

[29] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; see also FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[30] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

alerting the individual that this is happening. Facebook causes the browser to secretly duplicate the communication with Advocate, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

50. For example, if the user clicks "Find a Doctor" and enters their Zip Code and the doctor's specialty, like "Addiction Medicine," this is information is shared with Facebook, Google, or others that Defendant has configured its Pixel to interact with.

51. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

52. Every time Advocate sends a patient's website activity data to Facebook, that patient's personally identifiable information is also disclosed, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to the corresponding Facebook profile and the persons real world identity. A user who accesses Advocate's digital platforms while logged into Facebook will transmit the user cookie to Facebook, which contains that user's unencrypted Facebook ID. U

53. Google and other companies likewise process this data in a similar manner and use it to connect the information to particular individuals to build marketing and other data profiles.

54. Through the Pixel, Defendant Advocate shares its patients' identities and online activity, including personal information and search results related to their private medical treatment.

55. Defendant could have configured its tracking software to limit the information that it communicated to third parties but it did not and instead intentionally selected the features and functionality of the Pixel that resulted in the Data Breach.

56. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendant Advocate to disclose their Private Information and assist with intercepting their communications. Plaintiffs were never provided with any written notice that Defendant discloses its patients' protected health information, nor were they provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Plaintiffs' protected health information to Meta, Facebook, Google, and other unauthorized entities.

57. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

58. Defendant is required by law to maintain and safeguard Plaintiffs' protected health information and confidential communications. Advocate deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiffs' and Class Members' confidential communications, personally identifiable information, and protected health information; (2) disclosed patients' protected information to Facebook and others—unauthorized third-party eavesdroppers; and (3) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent. Plaintiffs did not discover that Advocate disclosed their personally identifiable information and protected health information to Facebook, and assisted Facebook with intercepting their communications

Plaintiff Deanna Danger's Experience

59. Plaintiff received healthcare services from one of the hospitals in Defendant's network and that relied on Defendant's digital healthcare platforms to communicate confidential patient information.

60. Plaintiff accessed Defendant's digital tools to receive healthcare services from Defendant and at Defendant's direction and encouragement. Plaintiff reasonably expected that her online communications with Defendant were confidential, solely between herself and Defendant and that such communications would not be transmitted to or intercepted by a third party.

61. Plaintiff is also a Facebook user and visited Defendant's website and digital platforms while logged in to Facebook.

62. Plaintiff provided her Private Information to Defendant and trusted that the information would be safeguarded according to Advocate's privacy policies and state and federal law.

63. As described herein, Defendant sent Plaintiff's Private Information to Meta, Google, and others when she used Defendant's digital platforms to communicate healthcare and identifying information to Defendant.

64. Pursuant to the process described herein, Defendant assisted Facebook, Google, and others with intercepting Plaintiff's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Advocate facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

65. By failing to receive the requisite consent, Defendant breached confidentiality

and unlawfully disclosed Plaintiff's personally identifiable information and protected health information.

66. Since she began using Defendant's digital healthcare platforms, Plaintiff has received targeted medial advertising on social media related to medical treatment.

CLASS ALLEGATIONS

67. Plaintiff brings this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

68. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All persons Defendant identified as being among those individuals impacted by the Data Breach that occurred on or around October 20, 2022.

69. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

70. Plaintiffs reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

71. **Numerosity**, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are 3,000,000 individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

72. **Commonality**, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exists and predominates over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect Plaintiffs' and Class Members' Private Information;

b. Whether Defendant had duties not to disclose the Plaintiffs' and Class Members' Private Information to unauthorized third parties;

c. Whether Defendant had duties not to use Plaintiffs' and Class Members' Private Information for non-healthcare purposes;

d. Whether Defendant had duties not to use Plaintiffs' and Class Members' Private Information for unauthorized purposes;

e. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' Private Information;

f. Whether and when Defendant actually learned of the Data Breach;

g. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

i. Whether Defendant failed to properly implement and configure the tracking software on its digital platforms to prevent the disclosure of information compromised in the Data Breach;

j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

k. Whether Defendant engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiffs' and Class Members' Private Information;

73. **Typicality, Fed. R. Civ. P. 23(a)(3)**: Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's use and incorporation of the tracking software.

74. **Policies Generally Applicable to the Class**: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

75. **Adequacy, Fed. R. Civ. P. 23(a)(4)**: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

76. **Superiority and Manageability, Fed. R. Civ. P. 23(b)(3)**: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the

controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

77. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

78. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

79. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

80. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure and unlawful disclosure of the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

81. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

82. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Private Information;

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

83. Plaintiffs and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

84. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Defendant.

85. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its website and the communications platforms and services therein.

86. Plaintiffs and Class Members communicated sensitive and protected medical information and individually identifiable information that they intended for only Defendant to receive and that they understood Defendant would keep private.

87. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiffs and Class members is an intentional intrusion on Plaintiffs' and Class members' solitude or seclusion.

88. Plaintiffs' and Class members had a reasonable expectation of privacy given Defendant's representations, HIPAA Notice of Privacy Practices and Privacy Policy. Moreover, Plaintiffs and Class members have a general expectation that their communications regarding healthcare with their healthcare providers will kept confidential. Defendant's disclosure of private medical information coupled with individually identifying information is highly offensive to the reasonable person.

89. As a result of Defendant's actions, Plaintiffs and Class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

90. Plaintiffs and Class members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

91. Plaintiffs and Class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class members for the harm to their privacy interests as a result of its intrusions upon Plaintiffs' and Class members' privacy.

92. Plaintiffs and Class members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class members in conscious disregard of their rights. Such damages are needed to deter Defendant's from engaging in such conduct in the future.

93. Plaintiffs also seek such other relief as the Court may deem just and proper..

COUNT II
BREACH OF CONTRACT
(On behalf of Plaintiff and the Class)

94. Plaintiffs and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

95. Defendant required Plaintiffs and the Class Members to provide their Private Information, including names, email addresses, phone numbers, computer IP addresses, and emergency contact information, appointment information, and other content submitted into Defendant's website as a condition of their receiving healthcare services.

96. As a condition of utilizing Defendant's digital platforms and receiving services from Defendant, Plaintiff and the Class provided their Private Information and compensation for their medical care. In so doing, Plaintiffs and the Class entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in its Privacy Policies and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

97. Plaintiffs and the Class Members fully performed their obligations under the contract with Defendant.

98. Upon information and belief, Defendant's relevant privacy policies and representations require it to take appropriate steps to safeguard the Private Information entrusted to it by the Plaintiffs and Class Members.

99. Defendant breached these agreements, which directly and/or proximately caused Plaintiffs and Class Members to suffer damages, including nominal damages.

100. Defendant breached the contracts it made with Plaintiffs and the Class by failing to safeguard and protect their Private Information, and by failing to provide timely and accurate

notice to them that the Private Information was compromised as a result of the Data Breach.

As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and the Class have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities.

101. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

102. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

103. A relationship existed between Plaintiffs and the Class one the one hand and Defendant on the other in which Plaintiff and the Class put their trust in Advocate to protect the Private Information of Plaintiffs and the Class and Advocate accepted that trust.

104. Defendant Advocate breached the fiduciary duty that it owed to Plaintiffs and the Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, and intentionally disclosing, the Private Information of Plaintiffs and the Class.

105. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiffs and the Class.

106. But for Defendant's breach of fiduciary duty, the damage to Plaintiffs and the Class would not have occurred.

107. Defendant's breach of fiduciary duty contributed substantially to producing the

damage to the Plaintiffs and the Class.

108. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiffs and Class Members are entitled to and do demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT IV
VIOLATION OF CONFIDENTIALITY OF PATIENT HEALTH CARE RECORDS
Wis. Stat. § 146.81 *et seq.*
(On Behalf of Plaintiff and the Class)

109. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

110. Under Wisconsin law all patient health care records must remain confidential and patient health care records may only be released to a person upon the informed consent of the patient, or as authorized by the patient.

111. Defendant disclosed the private and protected medical information of Plaintiffs and Class Members to unauthorized third parties without their knowledge, consent, or authorization.

112. Advocate is a healthcare provider as defined by Wis. Stat. Ann. § 146.816(1).

113. Plaintiffs and Class Members are patients, and, as a health care provider, Advocate had and has an ongoing obligation not to disclose their Private Information.

114. The Private information disclosed by Defendant is protected health information as defined by Wis. Stat. Ann. § 146.816(f).

115. Defendant violated Wis. Stat. § 146.81, *et seq* through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the Class. Defendant's conduct with respect to the disclosure of its patients confidential Private Information was willful and knowing because Defendant configured and implemented the

digital platforms and tracking software that gave rise to the Data Breach.

116. Plaintiffs and Class Members were injured as a result of Advocate's violation of the confidentiality of patient health care law.

117. As a result of its intentional and willful disclosure of Plaintiffs and Class Members' Private Information, Defendant is liable for actual damages, additional damages of at least $25,000 if the violation was willful or $1,000 otherwise, and the costs and attorneys' fees incurred as a result of the violation. Wis. Sta. Ann. § 146.84.

COUNT V
Wisconsin Deceptive Trade Practices Act, Wis. Stat. §§ 100.18, *et seq.*,
(On Behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

118. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

119. Defendant's conduct violates Wisconsin's Deceptive Trade Practices Act, Wis. Stat. §100.18 (the "WDTPA"),[23] which provides that no,

> "firm, corporation or association ... with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale ... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public ... which ... contains any assertion, representation or statement of fact which is untrue, deceptive or misleading."

120. Plaintiff and Class Members "suffered pecuniary loss because of a violation" of the WDTPA. Wis. Stat. §100.18(11)(b)(2).

121. Defendant deliberated engaged in deceptive an unlawful practices on or around April 28, 2022 when Defendant continued to claim on its website that "We maintain commercially reasonable security measures to protect [Private Information] we collect and store from loss, misuse, destruction, or unauthorized access." Specifically, Defendant continued to

make this claim even though Defendant knew its network had been accessed via the Data Breach.

122. Defendant further violated the WDTPA by: (a) fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access; (b) misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, so as to safeguard Private Information from unauthorized access; (c) omitting, suppressing, and concealing the material fact of the inadequacy of the security practices and procedures; (d) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access; and (e) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the First Data Breach to enact reasonable security practices to safeguard its systems and data from cyberattacks like the Data Breaches.

123. The purpose of Defendant's misrepresentations set forth herein was to minimize the harm and injury-in-fact Plaintiffs and Class Members are facing caused by the Data Breach, and therefore increase the sales and use of Defendant's goods and services.

124. Defendant knew or should have known that its computer systems and security practices and procedures were inadequate and that risk of the Data Breaches and theft was high.

Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

125. The Plaintiffs and the Class Members relied upon Defendant's deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the court deems proper. Wis. Stat. §§ 100.18(11)(b)(2) and 100.20(5).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and Plaintiffs' counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Sensitive Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant's to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and

statutory penalties, in an amount to be determined, as allowable by law; For an award of punitive damages, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) Pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: November 3, 2022

Respectfully Submitted,

/s/ Bryan L. Bleichner

Bryan L. Bleichner (MN Bar # 0326689)
Philip J. Krzeski (MN Bar # 0403291)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Attorneys for Plaintiff and the Putative Class